REMARKS

The Office Action dated July 8, 2008 has been received and carefully noted. The above amendments to the claims, and the following remarks, are submitted as a full and complete response thereto.

Please amend claims 1-3, 5, 6, 8, 9, 22, 28, 30, 34, 35, 48; and 49; please cancel claims 10-21 without prejudice or disclaimer; and please add new claims 50 and 51 as follows.

Claims 1-3, 5, 6, 8, 9, 22, 28, 30, 34, 35, 48; and 49 have been amended to more particularly point out and distinctly claim the subject matter of the invention. Claims 10-21 have been cancelled without prejudice or disclaimer and claims 50 and 51 have been added. No new matter is believed to have been added. Claims 1-51 are currently pending and are respectfully submitted for consideration.

Reconsideration and withdrawal of the objections and rejections is respectfully requested in light of the following remarks.

Claims 1-5, 8-15, 19, 21, 22-26, 29, 31, 32, 34-38, 42-44, 46, 48, and 49 were rejected under 35 U.S.C. § 102(e) as being anticipated by Shaw (U.S. Patent No. 7,058,970) ("Shaw"). The Office Action asserted that Shaw discloses all of the elements recited in claims 1-5, 8-15, 19, 21, 22-26, 29, 31, 32, 34-38, 42-44, 46, 48, and 49. However, this assertion by the Office Action is respectfully traversed as follows.

Claim 1, upon which claims 2-8 are dependent, recites an apparatus. The apparatus includes a proxy configured to receive a request for network services by at least

one remote network device and to perform a security integrity scanning operation on the requesting remote network device. The security scanning operation is performed before and after the remote network device signs on to the proxy. The apparatus also includes an authorization processor and access rules controller configured to determine if the remote network device is authorized to access the requested network services based on the results of the security scanning operation.

Claim 9 recites a system. The system includes at least one remote network device configured to access a network via a network connection to make a request for one or more network resident services. The system also includes a gateway configured to receive the request for services and perform a security integrity scanning operation on the remote network device prior to allowing access to the requested network services. The security scanning operation is performed before and after the remote network device signs on to the gateway. The system includes an authentication server configured to verify user authentication credentials of users of remote network that access the network. The system includes at least one network server configured to provide requested network services to at least one remote network accessing the network through the gateway.

Claim 22, upon which claims 23-34, are dependent, recites a method. The method includes performing scanning process and reporting result used in scanning script, including at least one variable defined to be used as a vehicle to convey results of a scanning process. The method also includes performing at least one scanning operation on the remote network device to verify a security integrity of the remote device. The

scanning operation is performed before and after the remote device signs on to a gateway device which is configured to perform the scanning operation. The method includes providing the results of the scanning operation for purposes of determining whether or not the remote network device is authorized to access the requested network services.

Claim 35, upon which claims 36-48 are dependent, recites a method. The method includes defining at least one access control policy for accessing network services wherein the access control policy depends, at least in part, on the results of an integrity scan performed on a remote network device. The method includes specifying what scan scripts are to be used under what conditions to the remote network device. The method also includes receiving at least one result of an integrity scan from the remote network device at a gateway device. The integrity scan is performed before and after the remote device signs on to the gateway device. The method includes regulating access by the remote network device to network services via the gateway device based, at least in part, on the results of the integrity scan.

Claim 49 recites an apparatus. The apparatus includes a proxying means for receiving a request for network services by at least one remote network device and to perform a security integrity scanning operation on the requesting remote network device. The security scanning operation is performed at least before the remote network device signs on to the proxy. The apparatus includes an authorization processing means and access rules controlling means for determining if the remote network device is authorized

to access the requested network services based on the results of the security scanning operation.

As will be discussed below, Applicants respectfully submit that Shaw fails to disclose, either expressly or inherently, all of the elements of the claims, and therefore fails to provide the advantages and features as discussed above.

Shaw generally discusses a network security authority system that provides on-connect scan and delivery in a virtual lobby to enforce security requirements for a network (see Shaw, Abstract). In the Response to Arguments section, the Office Action asserted that Figure 5; Column 4, Lines 50-64 and Figure 7; Column 6, Lines 33-47 of Shaw discloses throughout the specification various embodiments that allow the client to connect to the network via proxy device such as scanning for viruses *before* ***or*** *after* logging in (emphasis added) (see Office Action, Page 2, Lines 16-20). Contrary to the assertion made by the Office Action, Figure 6; Column 4, Lines 50-64 and Figure 7; Column 6, Lines 33-47 of Shaw fail to disclose, either expressly or implicitly, "a scanning operation is performed before ***and*** after the remote network device signs on to the proxy" (emphasis added), as recited in claim 1, and as similarly recited in claims 9, 22, 35, and 49.

Rather, Column 4, Lines 50-64 of Shaw, which corresponds to Figure 6 of Shaw, states:

> [t]he client 604 is scanned to determine if the client complies with security requirements 606. Connection is permitted to the network only if the client 604 complies with the security requirements 606.

> In another embodiment, the method further comprises interfacing with at least one provider 608 of at least one security mechanism to bring the client 604 into compliance with the security requirement, if the client is not in compliance. For example, delivery of one security mechanism is provided by a website of a vendor and patches are located on storage mediums on the network. Example embodiments redirect the client 604 to the website, verify installation status, and then install the patches. Then, a rescan reveals the client meets the security requirements and is provided access to the network.

Stated another way, Column 4, Lines 50-64 of Shaw is merely concerned with scanning to determine if the client is in compliance with the security requirements prior to providing access to the network, and if the client is not in compliance, then updating the client and rescanning prior to providing access to the network. In either scenario, nothing is disclosed in Column 4, Lines 50-64 of Shaw that remotely suggests "the security scanning operation is performed ***before and after*** the remote network device signs on to the proxy" (emphasis added), as recited in claim 1, and as similarly recited in claims 9, 22, 35, and 49.

Furthermore, Figure 7 of Shaw illustrates an alternative embodiment to Figure 6, as discussed above, for on-connect security scan and delivery. More particularly, Column 6, Lines 35-47 of Shaw, which corresponds to Figure 7 of Shaw, states:

> [t]he network security authority comprises a scanning component 702, a delivery component 704 and a repository component 706. The network security operates to scan the client 708 and deliver any security mechanism needed by the client 708 to comply with security requirements. Fig. 7 shows some example security mechanisms and configurations. In this case, the client has a virus scanner 710, a software firewall 712, and intruder detection system (IDS) 714, and other custom security mechanisms 716. the virus scanner is configured to check for the particular virus "I love you" 718 and other configurations 720 are also shown in Fig. 7 on the client 708.

Stated another way, Figure 7 of Shaw and Column 6, Lines 35-47 of Shaw are merely concerned with providing an on-connect security scan system. However, nothing is disclosed in Shaw that remotely suggests that "the security scanning operation is performed ***before and after*** the remote network device signs on to the proxy" (emphasis added), as recited in claim 1, and as similarly recited in claims 9, 22, 35, and 49.

Moreover, as admitted in the Response to Arguments section, the Office Action acknowledged that "Shaw discloses throughout the specification various embodiments that allow the client to connect to the network via proxy device such as scanning for viruses *before* ***or*** *after* logging in" (see Office Action, page 2, Lines 18-21). As such, it is well know that an "or" operation is not the same as an "and" operation. Therefore, as admitted by the Office Action, Applicants respectfully submit that Shaw cannot disclose, either expressly or inherently, in part that "the security scanning operation is performed ***before and after*** the remote network device signs on to the proxy" (emphasis added), as recited in claim 1, and as similarly recited in claims 9, 22, 35, and 49.

Accordingly, Applicants respectfully requests that the rejection of independent claims 1, 9, 22, 35, and 49 be withdrawn and these claims be allowed for at least the reasons stated above.

Furthermore, Applicants respectfully request that the rejection of claims 2-5, 8, 10-15, 19, 21, 23-26, 29, 31, 32, 34, 36-38, 42-44, 46, and 48 be withdrawn and these claims be allowed for at least the same reasons as their respective base claims, from which they depend, and for the specific limitations recited therein.

Claims 6, 7, 16-18, 27, 28, 30, 40, 41, and 45 were rejected under 35 U.S.C. §103(a) as being unpatentable over Shaw in view of Ji, *et al.* (U.S. Patent No. 6,728,886) ("Ji"). Particularly, the Office Action asserted that the combination of Shaw and Ji disclosed all of the elements of claims 6, 7, 16-18, 27, 28, 30, 40, 41, and 45. However, this assertion by the Office Action is respectfully traversed as followed.

Shaw is discussed above. Ji generally discusses distributed virus scanning arrangements. More particularly, Ji discusses techniques to permit a host computer to perform its own virus scanning on HTTP transferred data using executables downloaded to its browser upon startup (see Ji, Column 1, Lines 10-14). According to Ji, if the auto-config script detects that the browser is not capable of supporting local virus scanning, the auto script directs that all HTTP transfers be performed through a scan engine disposed centrally in order to allow virus scanning to be performed at the central server (see Ji, Column 7, Lines 31-37).

However, nothing is found or cited in Ji that cures the above-mentioned deficiencies of Shaw. For example, nothing is disclosed in Ji that remotely suggests "the security scanning operation is performed before and after the remote network device signs on to the proxy", as recited in claim 1, and as similarly recited in claims 9, 22, 35, and 49.

Therefore, Applicants respectfully submit that the subject matter disclosed in claims 6, 7, 16-18, 27, 28, 30, 40, 41, and 45 be allowed for at least the same reasons as

their respective base claims, from which they depend, and for the specific limitations recited therein. Accordingly, withdrawal of the rejection is respectfully requested.

Claims 6, 7, 16-18, 27, 28, 30, 40, 41, and 45 were rejected under 35 U.S.C. §103(a) as being unpatentable over Shaw in view of Hiltgen (U.S. Patent Publication No. 2003/0177392). Particularly, the Office Action asserted that the combination of Shaw and Hiltgen disclosed all of the elements of claims 6, 7, 16-18, 27, 28, 30, 40, 41, and 45. However, this assertion by the Office Action is respectfully traversed as followed.

Shaw is discussed above. Hiltgen generally discusses a secure user authentication over a communication network. More particularly, Hiltgen discusses a server infrastructure and a network system that enables secure user authentication using a network client having access via card reader to a smart card (see Hiltgen, Paragraph [0002]). However, nothing is found or cited in Hiltgen that cures the above-mentioned deficiencies of Shaw. For example, nothing is disclosed in Hiltgen that remotely suggests "the security scanning operation is performed before and after the remote network device signs on to the proxy", as recited in claim 1, and as similarly recited in claims 9, 22, 35, and 49.

Therefore, Applicants respectfully submit that the subject matter disclosed in claims 6, 7, 16-18, 27, 28, 30, 40, 41, and 45 be allowed for at least the same reasons as their respective base claims, from which they depend, and for the specific limitations recited therein. Accordingly, withdrawal of the rejection is respectfully requested.

Claim 50 is a new claim, which recites features similar to those recited in independent method claim 22. Claim 50 recites a computer program, embodied on a computer-readable medium, configured to control a processor to implement a method. The method includes performing scanning process and reporting result used in scanning script, including at least one variable defined to be used as a vehicle to convey results of a scanning process. The method includes performing at least one scanning operation on the remote network device to verify a security integrity of the remote device. The scanning operation is performed before and after the remote device signs on to a gateway device which is configured to perform the scanning operation. The method includes providing the results of the scanning operation for purposes of determining whether or not the remote network.

Applicants respectfully submit that none of the references, relied upon by the Office Action, whether considered alone or in combination, disclose, either expressly, implicitly or inherently, all of the elements of claim 50. For example, none of the references remotely suggest, in part "the scanning operation is performed before and after the remote device signs on to a gateway device which is configured to perform the scanning operation", as recited in claim 50.

Claim 51 is a new claim, which recites features similar to those recited in independent method claim 35. Claim 51 recites a computer program, embodied on a computer-readable medium, configured to control a processor to implement a method. The method includes defining at least one access control policy for accessing network

services wherein the access control policy depends, at least in part, on the results of an integrity scan performed on a remote network device. The method also includes specifying what scan scripts are to be used under what conditions to the remote network device. The method includes receiving at least one result of an integrity scan from the remote network device at a gateway device. The integrity scan is performed before and after the remote device signs on to the gateway device. The method includes regulating access by the remote network device to network services via the gateway device based, at least in part, on the results of the integrity scan.

Applicants respectfully submit that none of the references, relied upon by the Office Action, whether considered alone or in combination, disclose, either expressly, implicitly or inherently, all of the elements of claim 51. For example, none of the references remotely suggest, in part "integrity scan is performed before and after the remote device signs on to the gateway device", as recited in claim 51.

Accordingly, Applicant respectfully submit that the subject matter of claims 50 and 51 are allowable for reasons similar to those discussed above.

For at least the reasons discussed above, Applicants respectfully submit that none of the cited references, whether considered alone or in combination, disclose, either expressly, implicitly or inherently, all of the elements of the claimed invention. These distinctions are more than sufficient to render the claimed invention unanticipated and unobvious. It is therefore respectfully requested that all of claims 1-51 be allowed, and this application passed to issue.

If for any reason the Examiner determines that the application is not now in condition for allowance, it is respectfully requested that the Examiner contact, by telephone, the applicants' undersigned attorney at the indicated telephone number to arrange for an interview to expedite the disposition of this application.

In the event this paper is not being timely filed, the applicants respectfully petition for an appropriate extension of time. Any fees for such an extension together with any additional fees may be charged to Counsel's Deposit Account 50-2222.

Respectfully submitted,



Sheetal S. Patel
Attorney for Applicants
Registration No. 59,326

Customer No. 32294
SQUIRE, SANDERS & DEMPSEY L.L.P.
14th Floor
8000 Towers Crescent Drive
Vienna, Virginia 22182-6212
Telephone: 703-720-7800
Fax: 703-720-7802

SSP:dk

Enclosures: Additional Claim Fee Transmittal
Check No. 19750